

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-259011

(43)Date of publication of application : 16.09.1994

(51)Int.Cl. G09C 1/00
H04L 9/06
H04L 9/14

(21)Application number : 05-042591

(71)Applicant : NIPPON TELEGR & TELEPH
CORP <NTT>

(22)Date of filing : 03.03.1993

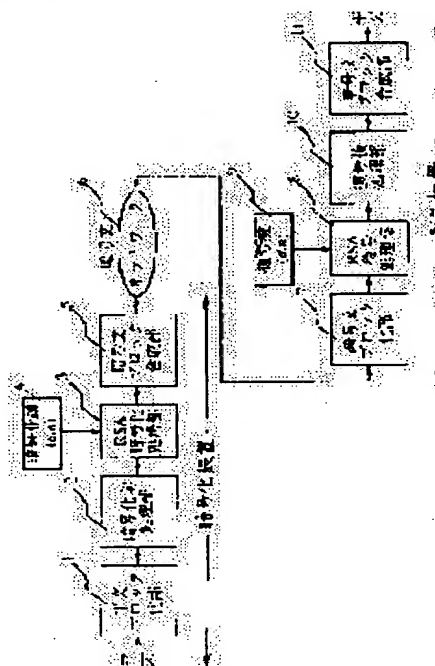
(72)Inventor : ISHII SHINJI
MATSUMOTO HIROYUKI

(54) ENCIPHERING DEVICE AND DECODER FOR OPEN KEY

(57)Abstract:

PURPOSE: To make a ciphertext hard to be deciphered by excluding specific plaintexts 0, 1, and $n-1$ which become the same texts as the original plaintext even after RSA ciphering.

CONSTITUTION: A plaintext block division part 1 divides an input plaintext into plaintext blocks of integers between 0 and $n-3$, a enciphering preprocessing part 2 adds two to the respective plaintext blocks, and an RSA enciphering processing part 3 enciphers only blocks of integers between 2 and $n-2$ by utilizing an key (e, n). On a decoding side, an RSA decoding processing part 8 deciphers the respective ciphertext blocks by utilizing a decoding key (d, n), a decoding postprocessing part 10 subtracts two from the decoding plaintexts, and the results are connected in order to obtain the original plaintext.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 6 - 2 5 9 0 1 1

(43) 公開日 平成 6 年 (1994) 9 月 16 日

(51) Int. Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G09C 1/00		8837-5L		
H04L 9/06				
9/14				
		7117-5K	H04L 9/02	2

審査請求 未請求 請求項の数 2 . O L (全 5 頁)

(21) 出願番号 特願平 5 - 4 2 5 9 1

(22) 出願日 平成 5 年 (1993) 3 月 3 日

特許法第 30 条第 1 項適用申請有り 1993 年 1 月 2 日、社団法人電子情報通信学会発行の「電子情報通信学会技術研究報告 Vol. 92 No. 439」に発表

(71) 出願人 0 0 0 0 0 4 2 2 6

日本電信電話株式会社

東京都千代田区内幸町一丁目 1 番 6 号

(72) 発明者 石井 晋司

東京都千代田区内幸町 1 丁目 1 番 6 号 日

本電信電話株式会社内

(72) 発明者 松本 博幸

東京都千代田区内幸町 1 丁目 1 番 6 号 日

本電信電話株式会社内

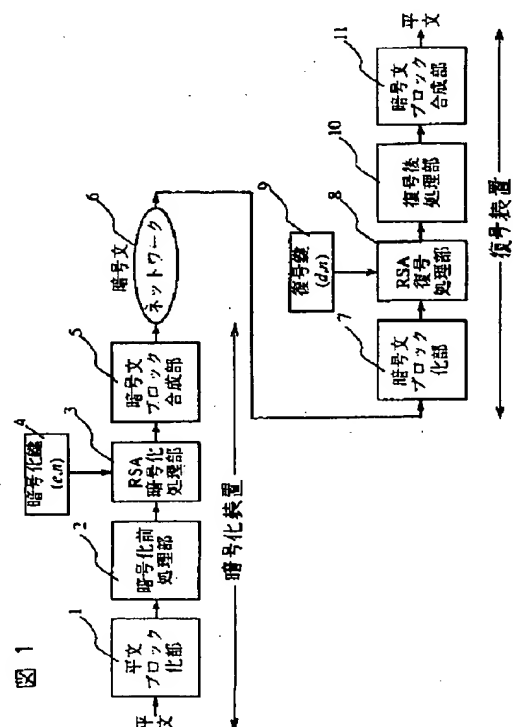
(74) 代理人 弁理士 草野 卓

(54) 【発明の名称】 公開鍵暗号化装置および復号装置

(57) 【要約】 (修正有)

【目的】 RSA 暗号化しても元の平文と同一となる特定の平文 0, 1, $n-1$ を除外して、解読され難くする。

【構成】 平文ブロック化部 1 で入力平文を 0 以上 $n-3$ 以下の整数の平文ブロックに分割し、暗号化前処理部 2 でその各平文ブロックに 2 を加算して 2 以上 $n-2$ 以下の整数のブロックにつき、この各ブロックを RSA 暗号化処理部 3 で鍵 (e, n) を利用して暗号化する。復号側ではその各暗号文ブロックを RSA 復号処理部 8 で復号鍵 (d, n) を利用して復号し、その復号された各平文から 2 を復号後処理部 10 で引算し、その結果を次に順次連続させて元の平文に戻す。



1

2

【特許請求の範囲】

【請求項 1】 乗および法 n の剰余演算を利用する公開鍵暗号装置において、

0 以上 $n - 3$ 以下の整数で表現された平文に 2 を加える暗号化前処理手段と、

その暗号化前処理手段によって加算された平文 2 以上 $n - 2$ 以下の整数で表現された暗号文に暗号化する平文暗号化手段と、

を具備する公開鍵暗号化装置。

【請求項 2】 乗および法 n の剰余演算を利用する公開鍵復号装置において、

2 以上 $n - 2$ 以下の整数で表現された暗号文を平文に戻す暗号文復号手段と、

その暗号文復号手段で復号された平文から 2 を引いて正規の平文を得る復号後処理手段と、

を具備する公開鍵復号装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 この発明は、RSA 暗号で知られている乗（べき）乗および剰余演算を利用する公開鍵暗号アルゴリズムを利用する暗号化装置および復号装置に関するものである。

【0002】

【従来の技術】 乗および剰余演算を利用する公開鍵暗号アルゴリズムの代表として、RSA 暗号が知られている。（RSA 暗号の詳細な説明は、社団法人電子情報通信学会発行現代暗号理論第 6 章等を参照のこと）。RSA 暗号では、暗号化側が、暗号化指数 e 、法 n を利用して整数で表現された平文 M を暗号化する。一方復号側は、復号指数 d 、法 n を利用して暗号文 D をもとの平文 M に戻す。RSA 暗号は、アルゴリズムの特徴から、平文 M は、 $0 \leq M \leq n - 1$ の整数に限られている。

【0003】 暗号化した結果が元の平文と一致する平文 M つまり暗号化できない平文 M が必ず 9 組あることが指摘されている（参考文献：社団法人電子情報通信学会発行現代暗号理論第 6 章 pp. 114 - 116）。しかし、従来は、実システムでは n は 2 の 512 乗程度であることから、前記 9 組が出現する確率は $9/2^{512}$ と極めて小さいので特に重要視されていなかった。

【0004】

【発明が解決しようとする課題】 しかし、これらの 9 組中の 3 組は、特定の平文で、0, 1, $n - 1$ である。この 0, 1 は暗号化指数 e 、復号指数 d 、法 n に依存せず、 $n - 1$ は法 n のみに従属な値である。したがって、どのような暗号化指数 e 、復号指数 d 、法 n を選択したとしても、悪意を持つ盗聴者はこれらの 3 組の平文 M を、部分解読できる。

【0005】 たとえば、法 n 以上の平文を暗号化する場合、ある図形や文字の書かれた資料をスキャナ（画像読み取り器）を使って 2 値データとして読み込むと、連

続した 0 が数千ビット続くこともしばしばある。このようなデータを、RSA 暗号を利用して暗号化しても、暗号文はもとの平文と全く同じ連続した 0 が数千ビットになってしまう。

【0006】 この発明の目的は、どのような鍵（暗号化指数 e 、復号指数 d 、法 n ）を選んだとしても暗号化結果が必ず元の平文と同じになる組み合わせがない公開鍵暗号装置及びその復号装置を提供することにある。

【0007】

【課題を解決するための手段】 請求項 1 の発明によれば 0 以上 $n - 3$ 以下の整数で表現された平文を補正定数加算手段により 2 が加算され、その加算された平文が平文暗号化手段で乗及び法 n の剰余演算を利用して暗号化される。請求項 2 の発明によれば 2 以上 $n - 1$ 以下の整数で表現された暗号文が暗号文復号手段で乗及び法 n の剰余演算を利用して平文に復号され、補正定数減算手段によりその復号された平文から 2 が引算されて正規の平文とされる。

【0008】

【作用】 平文は 0 以上 $n - 3$ 以下の整数で表現され、これに 2 が加算され、つまり平文は 2 以上 $n - 1$ の整数となり、この加算された平文が暗号化されるため、暗号化直前の平文には 0, 1 は含まれない、つまり暗号化しても元の平文となる平文 0 と 1 は除外される。それだけ、暗号化しても元の平文となる特定平文の暗号化が避けられ、その特定平文の部分解読が避けられる。なお特定平文 $n - 1$ も除外して暗号化するには、最初に平文を 0 以上 $n - 4$ 以下の整数で表現すればよい。

【0009】

【実施例】 この発明の実施例の概要を述べる。最初に、 $n - 3$ 以上の整数を、あらかじめ 0 以上 $n - 4$ 以下の複数のデータブロックに分割する。このようにして、すべての正整数を 0 以上 $n - 4$ 以下の整数に分割して、その後すべてのデータブロックに 2 を加える。つぎに、2 以上 $n - 2$ 以下のデータブロックに分割することにより、すべての正整数を特定平文を避けて暗号化できるようにする。

【0010】 この発明の暗号化装置および復号装置を用いた公開鍵暗号システムを図 1 に示す。この発明を実現するために従来装置に対して新たに加わる部分は、暗号化前処理部 2 と復号後処理部 10 のみで、そのほかは従来の RSA 暗号装置と全く同じである。なお、デジタル信号は、通常 2 進数で表現するため、この実施例も 2 進数を前提として記述する。

【0011】 暗号化装置では暗号化しようとするデータ（平文）を平文ブロック化部 1 に入れる。平文ブロック化部 1 では、最初にデータを 0 以上 $n - 4$ 以下のデータブロックに分割する。平文ブロック化部 1 の処理動作を図 2 を参照して説明する。まず j を 1 とし (S_j)、次に入力平文の先頭から k ビットを取り出して M_j とする

(S_i)。その M_i が $n-3$ より小さいかを調べ(S_i)、 $n-3$ より小さければその M_i を j 番目の平文ブロックとする(S_i)。 M_i が $n-3$ より小でなければ、その M_i の再下位ビットを残りの平文の先頭に戻し(S_i)、 M_i を1ビット下位側(右側)にシフトし、つまり、 M_i を2分の1として(S_i)、ステップ S_i に移り、その M_i を j 番目の平文とする。次に j を $+1$ してステップ S_i に戻る(S_i)。

【0012】このようにして得られた、 $0 \sim n-4$ の整数の k ビットの平文ブロック M は、暗号化前処理部2でそのすべてのデータブロックに2を加え、図3Aに示すように各平文ブロック M の値2だけずらされる。これにより平文ブロック M ($2 \leq M \leq n-2$)が完成する。この平文ブロック M は、従来のRSA暗号と同じ方法により、RSA暗号化処理部3で暗号化鍵(e, n)を利用して暗号化し、暗号文 D ($2 \leq D \leq n-2$)を得る。

【0013】このとき暗号文 D のビット数は、2ビットから k ビットまで、ばらばらのビット長になる。データをこのまま複数の暗号文 D を連続して送信してしまうと、受信側では、どこが暗号文の切れ目であるかわからないために、復号できない。そこで、もっともビット長の長い k ビットにそろえるために、 k ビットに満たない暗号文には、 k ビットになるように上位ビットに0を加える。このようにすることにより、暗号文 D は、すべて、 k ビットの暗号文ブロックとなる。この暗号文ブロックは、 k ビットであるが、上位ビットに0が詰まっているだけなので暗号文ブロックも暗号文 D と同じ暗号文ブロック D ($2 \leq D \leq n-2$)とあらわすことができる。

【0014】暗号文ブロック合成部5では、暗号化データのビット長を k ビットに整え、暗号文ブロック D とし、その暗号文ブロック D を合成してネットワーク6を介して受信側に伝達する。受信側の復号装置は、受け取った暗号文を暗号文ブロック化部7に取込む。暗号文ブ

ロック化部7では、受け取った暗号文を k ビットごとの暗号文ブロックに区切る。暗号文ブロックは、従来の復号と全く同じ方法で、RSA復号処理部8で復号鍵(d, n)9を利用して復号する。

【0015】つぎに、復号後処理部10では、復号した平文ブロックから2を引き、図3Bに示すように整数 $2 \sim n-2$ をそれぞれ2だけ小さい値にずらす。最後に、平文ブロック合成部11で平文ブロックを合成することにより元の平文に戻すことができる。補正定数の2は、盗聴者などに知られても、暗号強度には全く影響がない。したがって、補正定数は、誰もがいつでも2を使用しても何も問題はない。もちろん、暗号化側で、暗号文の送信の前に2をヘッダとして付与したり、2を使用することを公開してもかまわない。上述では平文をまず $0 \sim n-4$ の整数のブロックにしたが、平文を $0 \sim n-3$ の整数のブロックに分割しても、通常は $n-3$ の平文ブロックが連続するようなことはないから、これに2を加算したブロックは $n-1$ で暗号文も $n-1$ となるが、全体として解読されるおそれはない。

【0016】

【発明の効果】従来の剰余を利用する公開鍵暗号アルゴリズムに共通した弱点の1つとして、どのような鍵を選んでも一部の暗号文は容易に解かれてしまう性質があった。しかしこの発明は、このような一部の暗号文をさけて暗号化することにより、どのような鍵を選んでも一部の暗号文が容易に解かれることを防ぐことができる。

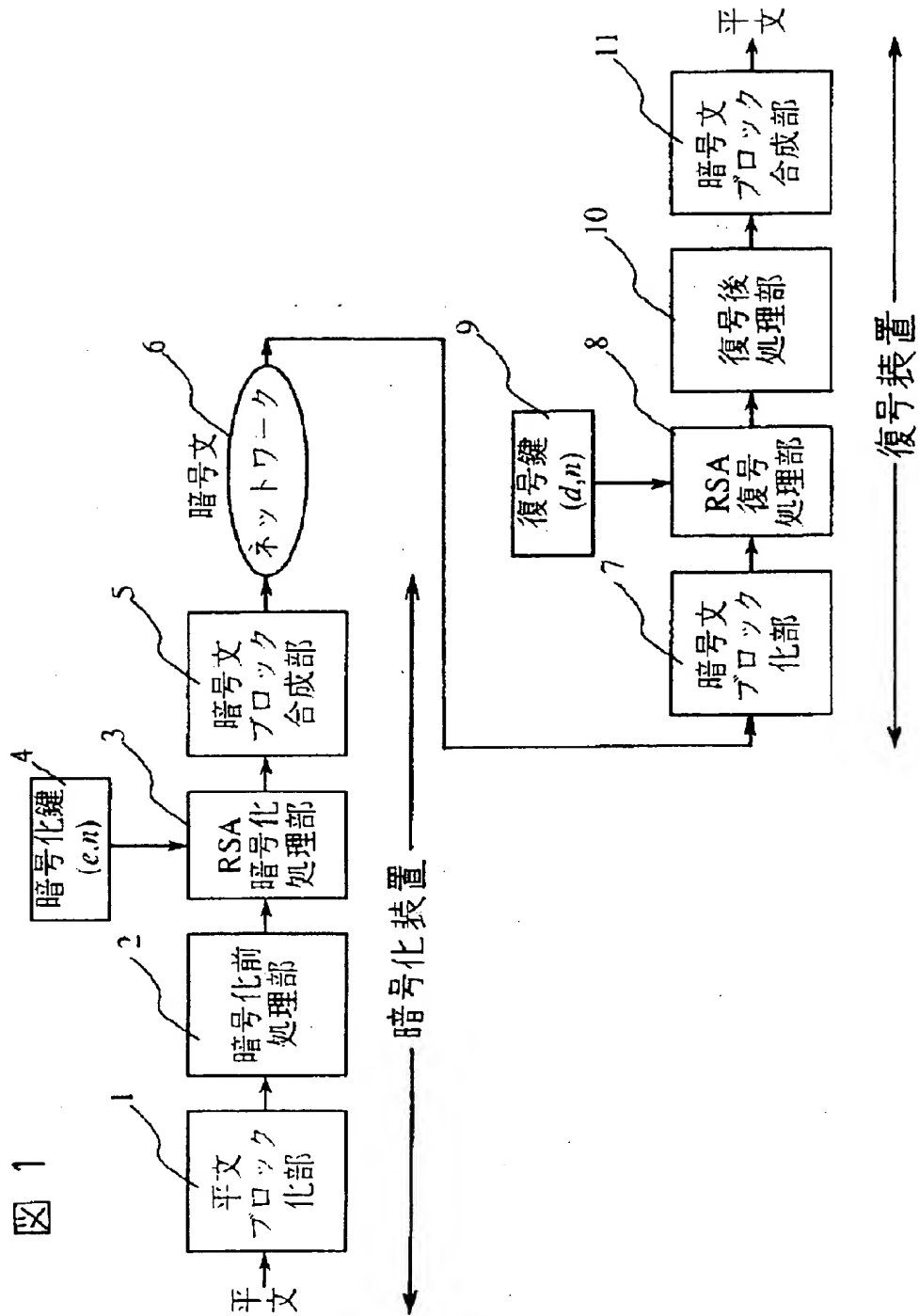
【図面の簡単な説明】

【図1】この発明の実施例の全体を示すブロック図。

【図2】十分長い平文をブロック化するための処理例を示す流れ図。

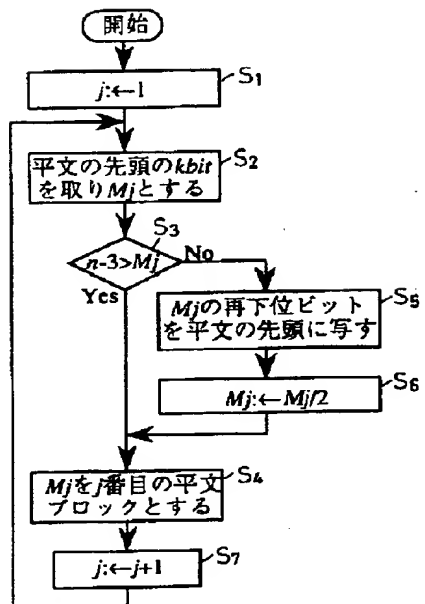
【図3】Aは図1中の暗号化前処理部2の内部動作を具体的に説明する図、Bは図1中の復号後処理部10の内部動作を具体的に説明する図である。

【 図 1 】



【図 2】

図 2



【図 3】

図 3

